

eCopy ShareScan® 5.0

Installation Guide

for Ricoh devices



Licensing, Copyright, and Trademark information

The information in this document is subject to change and does not represent a commitment on the part of Nuance Communications, Inc. The software described in this document is furnished under a license agreement. The software may be used or copied only in accordance with the terms of the agreement. It is against the law to copy the software on any medium except as specified in the license agreement. No part of this document may be reproduced, transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, or translated into any language for any purpose other than the purchaser's personal use, without the written permission of Nuance Communications, Inc.

© 2012 Nuance Communications. All Rights Reserved.

Nuance, the Nuance logo, eCopy PaperWorks and OmniPage are trademarks or registered trademarks of Nuance Communications, Inc. or its affiliates in the United States and/or other countries. All other trademarks referenced herein are the property of their respective owners.

Open Text, eDOCS, Open Text Fax Server, and RightFax are registered trademarks or trademarks of Open Text Corporation in the United States and/or other countries.

EMC, Documentum, and ISIS are registered trademarks of EMC Corporation.

IBM, Lotus, Lotus Notes, and Lotus Domino are trademarks and/or registered trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries or both.

Intel and Pentium are registered trademarks of Intel Corporation.

Microsoft, Windows, Windows NT, Outlook, SharePoint, and MS-DOS are registered trademarks and Windows Server and Windows Vista are trademarks of Microsoft Corporation in the USA and in other countries.

Autonomy and the Autonomy logo, iManage, Interwoven, and WorkSite are registered trademarks or trademarks of Autonomy Corporation plc.

Ricoh is a registered trademark of Ricoh, Inc.

Customer Support services

Customer Support services include the following components:

- Customer support for licensing, registration, and other non-technical issues
- Technical support
- Hardware RMA (Return Merchandise Authorization), where applicable

Note:

Nuance Communications does not provide hardware support. Contact your hardware dealer/distributor, or system integrator for support information.

The support services are available to registered users of Nuance Communications software during the warranty period or for the duration of your software Maintenance and Support (M&S) agreement. Contact your supplier for details, as described in the M&S agreement.

The main Support page is at <http://support.nuance.com>, where you can obtain information about Customer Support services, hours of operation, contact information, policies, and process descriptions. In the list of products, select the eCopy product and then click **Go**. The Support Overview page opens.

In addition to support provided by your dealer or distributor, the Ask eCopy Web site provides 24x7 access to a knowledge base. To access Ask eCopy, click the link on the main Support page.

If you purchased your software directly from Nuance Communications, check Ask eCopy for solutions to your technical problems. If necessary, open a ticket from the Ask eCopy Web site.

Contact information

US/North America

Corporate Headquarters Telephone: +1.781.565.5000

Customer Support Services Telephone: +1.781.565.4600

Outside North America

Please contact your local dealer or national sales organization.

ShareScan Installation Guide

The eCopy ShareScan software extends the capabilities of digital copiers and scanners. When installing and setting up a ShareScan system, you must be familiar with the scanning devices that you will use with ShareScan, the ShareScan software components, and the basic installation and configuration workflow.

This guide is intended for administrators responsible for the initial installation, configuration, and licensing of ShareScan. For the device-specific Pre-Installation Checklist (PICL), see the relevant vendor-specific PICL. For information pertaining to the ShareScan (pre)install, see this guide. For configuration and Administration Console usage, refer to the Help (accessible via pressing **F1** on the Administration Console).

This document is written under the assumption that readers are familiar with working in a server-client architecture and environment.

In this guide:

ShareScan Installation Guide	1
1 - Pre-install considerations	4
1.1- System requirements for the ShareScan Manager PC	4
1.1.1 - Operating systems	4
1.1.2 - Virtual environments	5
1.1.3 - Memory Configuration	5
1.1.4 - Checklist for the ShareScan Manager PC	5
1.1.5 - Database rights	6
1.1.6 - Network	6
1.2- Support information	7
1.2.1 - Languages	7
1.2.2 - Supported devices	7
1.3- eCopy connectors	7
1.3.1 - eCopy connector for Microsoft Exchange (Mail and/or Fax)	8
1.3.1.1 - Supported versions:	8
1.3.1.2 - Installation prerequisites and suggestions	8
1.3.1.3 - Configuring MAPI/MAPI protocol for Exchange Mail and Fax connectors	8
1.3.1.4 - Exchange 2010 CAS support for MAPI protocol	8

1.3.2 - eCopy connector for IBM Lotus Notes (Mail and/or Fax).....	9
1.3.2.1 - Supported versions.....	9
1.3.2.2 - Installation prerequisites and suggestions.....	9
1.3.3 - eCopy connector for LDAP/SMTP (Mail and/or Fax).....	9
1.3.3.1 - Supported versions.....	9
1.3.3.2 - Installation prerequisites and suggestions.....	10
1.3.4 - eCopy Scan to Desktop.....	10
1.3.4.1 - Installation prerequisites and suggestions.....	10
1.3.5 - eCopy Quick Connect.....	11
1.3.5.1 - Supported versions.....	11
1.3.5.2 - Installation prerequisites and suggestions.....	11
1.3.6 - eCopy connector for OpenText Fax Server (RightFax Edition).....	12
1.3.6.1 - Supported versions.....	12
1.3.6.2 - Installation prerequisites and suggestions.....	12
1.3.7 - eCopy Scan to Printer.....	12
1.3.7.1 - Installation prerequisites and suggestions.....	12
1.3.8 - eCopy connector for Microsoft SharePoint.....	12
1.3.8.1 - Supported versions.....	12
1.3.8.2 - Installation prerequisites and suggestions.....	12
1.3.9 - eCopy connector for EMC Documentum.....	13
1.3.9.1 - Supported versions.....	13
1.3.9.2 - Installation prerequisites and suggestions.....	13
1.3.10 - eCopy connector for Autonomy iManage WorkSite.....	14
1.3.10.1 - Supported versions.....	14
1.3.10.2 - Installation prerequisites and suggestions.....	14
1.3.11 - eCopy connector for Open Text Content Server - eDOCS Edition.....	14
1.3.11.1 - Supported versions.....	14
1.3.11.2 - Installation prerequisites and suggestions.....	14
1.3.12 - eCopy connector for Open Text Content Server.....	15
1.3.12.1 - Supported versions.....	15
1.3.12.2 - Installation prerequisites and suggestions.....	15

2 - Installing ShareScan	16
2.1- Basic workflow	16
2.2- Installing ShareScan	16
2.2.1 - Custom database installation options	18
2.2.1.1 - No SQL is installed	18
2.2.1.2 - Only ShareScan is installed	18
2.2.1.3 - Only the ShareScan database and the SQL server are installed	18
2.3- Adding devices	18
2.4- Upgrading ShareScan	19
2.4.1 - Upgrading from ShareScan 4.x	19
2.4.2 - Upgrading ShareScan 5 with Service Packs	20
3 - Client-side installation	20
3.1- Installing the ShareScan Ricoh client	20
3.1.1 - Installing the ShareScan Ricoh client without remote installation	20
3.1.1.1 - For 32-bit systems	21
3.1.1.2 - For 64-bit systems	21
3.1.2 - Installing the ShareScan Ricoh client via the ShareScan Administration Console (recommended)	21
3.1.3 - To install the ShareScan Ricoh client via a Web browser	22
3.1.4 - To install the ShareScan Ricoh client from an SD card	23
3.1.5 - To uninstall the ShareScan Ricoh client via a Web browser	24
3.1.6 - To uninstall the ShareScan Ricoh client from a device	24
3.2- Installing a Ricoh ScanStation Driver	25
3.2.1 - ISIS drivers	25
4 - Licensing devices	26
4.1- Loading licenses	26
4.2- Activating licenses	27
4.3- Loading activated licenses	27
4.4- Reactivating licenses	27
4.5- Removing licenses	28
5 - ShareScan post-install	28

5.1- ScanStation post-install.....	28
5.2- Send to eCopy service.....	28
5.2.1 - Send to eCopy configuration options.....	29
5.2.1.1 - Configuration settings:.....	29
5.2.1.2 - Send to eCopy ShareScan settings.....	29
5.3- Configuring ShareScan (examples).....	30
5.3.1 - To configure a service (example – Activity Tracking):.....	30
5.3.2 - To configure an Extender (example – Forms Processing Extender):.....	30
5.3.3 - To configure a Quick Connect connector profile to use Forms Processing Extender data	31
5.3.4 - To test the configuration of a profile:.....	31
6 - Next steps.....	32
6.1- Best practices.....	32
6.2- Troubleshooting.....	33

1 - Pre-install considerations

The following chapter contains information on the various tasks to be performed prior to installing ShareScan, as well as the requirements that must be met before the product installation.

1.1- System requirements for the ShareScan Manager PC

1.1.1 - Operating systems

- Windows XP SP3 32-bit
- Windows Vista SP2 32-bit
- Windows 7 SP1 32-bit / 64-bit
- Windows Server 2003 SP2 32-bit
- Windows Server 2008 SP2 32-bit
- Windows Server 2008 R2 SP1 64-bit
- Latest version of .NET Framework 3.5 SP1 installed (Windows XP and Vista)
- The ShareScan Administration Console and the ShareScan Manager cannot be installed on Linux, Solaris or Macintosh operating systems.

1.1.2 - Virtual environments

- VMware ESX v4 and the ESX Server portion of VSphere v4
- VMware Workstation 6.5 or 6.5.5

1.1.3 - Memory Configuration

- 2 GB physical memory (minimum); 4 GB recommended (8 GB recommended for systems using 100+ MFPs)
- 5 GB disk space (including SQL server and prerequisites)

1.1.4 - Checklist for the ShareScan Manager PC

- Ensure you are about to install the ShareScan Manager to a dedicated PC (that is, a PC exclusively tasked with the running of the ShareScan Manager).
- Changing the name of the PC after installing ShareScan is not advised. If you must change the PC name, consult the licensing-related chapters of ShareScan Help for the necessary steps.
- Run the Automatic Updates before you start installing ShareScan. **Pay extra attention that you have Automatic Updates of the operating system TURNED OFF during the installation.**
- ShareScan 5.0 installs a customized Apache Tomcat web service. Already existing Tomcat installs are not supported.
- If you have multiple NIC cards, disable all but the one you will use for your ShareScan installation. From ShareScan Service Pack 4 onwards, this is not required, as you can use a registry setting to control which NIC is used by the Manager.
- The same limitation applies to virtual environments: the VM configuration should contain only a single network adapter bridged to a physical adapter that connects to the same network where the MFP devices and the backend systems are connected to. The hosting machine can have multiple physical NICs.
- For ScanStation platforms, you have to enter the IP address of the NIC card in the ScanStation configuration file (config.xml). You have to ensure that the IP address in the **SERVER manager** line is the same as the IP address given to the ShareScan Manager in the registry, and it must also correspond to the value of the **address** in config.xml.
- For virtual environment usage, ensure that your virtual drive type is IDE.
- Check if your drive format is NTFS.
- Ensure that Microsoft IIS is not installed or is not listening to the ports used by ShareScan (listed below).
- ShareScan 5.0 licenses are installed to a SQL Server to allow easy management of devices. Prior to installing ShareScan 5.0, it is important to determine if licenses will be managed individually from each ShareScan Manager, or if you would like to manage all licenses from a single SQL Server. The ShareScan installer can install a local copy of SQL Server 2008 R2 Express for managing licenses. It can also create the appropriate database structure on an existing SQL server for consolidated key management.
- ShareScan 5.0 license keys must be activated against a Nuance Activation Server. License keys can only be activated once, so inspect the setup carefully prior to activation. All license keys provide a 30-day grace period before activation is required to ensure the setup is as intended. Manual activation is available for servers that are unable to communicate directly with the Nuance Activation Server.

- If you plan to use the **Single Sign On** feature of the **Session Logon** service, ensure that the ShareScan Manager PC is a member of the domain for which Session Logon is configured.
- Check whether you have a working, installed Java runtime environment by running `java -version` via `cmd.exe`. If the command does not display a version number, (re)install Java runtime environment to make ShareScan client applications work properly. On Windows 7, you can use the **Start Menu > Control Panel > Uninstall a program** to check and update your Java version as necessary.
- Make sure you disable local firewalls. If you do not disable the firewalls, and the Manager PC is running Windows XP SP3, you must add the **ShareScanManager.exe**, **ShareScanAgent.exe**, **ShareScanAdminConsole.exe**, **InBoxAgent.exe**, and **SQLServer.exe** under the **Control Panel > Windows Firewall > Exception** tab.
- If you are planning to have firewalls enabled, leave the following ports open (between ShareScan Manager and the multifunction device):
 - **TCP**: 80, 443, 2121, 8005, 8009, 8080, 9030, 9200-9220, 9600, 9601, 50001, 50002
 - **UDP**: 161, 8125, 8899, 9988

If any of these ports are in use, ShareScan displays a warning. Ports in use do not block installation, but must be opened later for proper functionality.

1.1.5 - Database rights

- If you are about to deploy a database (either locally or remotely), check to see whether you have full rights/access to the location (through an "sa" account).
- Modifying an existing SQL database also requires full rights/access to the location via an "sa" account.
- If you are using an existing ShareScan SQL database and you cannot get an "sa" account (required for installation only), then you need to get a "named instance" of the SQL server created for your purposes.
- Ensure that your database is in the same domain as the ShareScan Manager.
- If you use your own SQL server installation, ensure that you use "mixed mode" authentication (that is, SQL Server Authentication plus Windows Integration). In case the SQL server is already installed, check if this type of authentication is in use. You can find the setting under **Server Properties**.

1.1.6 - Network

- **Domains and Workgroups:** ShareScan can be configured to run in either domain-based networks or workgroup environments. Windows 2003 or later domain environments are supported. For best performance, a single domain/workgroup is recommended (multiple domains/workgroups are also supported).
- **Subnets and VLANs:** The ShareScan Manager PC can be on different subnets or VLANs from the multifunction devices, provided that the multifunction devices can communicate with the Manager PC using an IP address. If your multifunction devices span multiple subnets or VLANs, a router is required to pass packets back and forth. However, in these situations the UDP and the SNMP based device discovery mechanisms may not be functional.
- **IP Addresses:** Use static IP addresses for both the ShareScan Manager PC and the MFPs. To change the IP address of the Manager PC: (a) remove all devices from the Manager, (b) change the IP address, and (c) reboot the Manager PC.
- **Gateway Address:** ShareScan does not require a gateway address.

- **Host Name:** The host name must not exceed 60 characters. Device host names are resolved using DNS. This happens once you have added a device and confirmed it. If the device is not registered in the DNS, then its name in the **Devices** tab (Administration Console) may change after confirmation.
Note that changing the host name after installation can cause licensing and database issues, and is therefore **not supported**.
- **Network Attached Storage Devices (NAS):** ShareScan 5.0 does not support NAS devices.
- **Novell:** ShareScan does not support direct communication between a ShareScan Manager PC and a multifunction device on Novell networks. However, when Novell client software is installed on the Manager PC some Connectors (eCopy Quick Connect, and the eCopy Scan to Desktop) can bridge to a Novell server. A Novell client must be installed on the ShareScan Manager PC if Novell authentication of Scan Inboxes is required.
The eCopy Connector for LDAP/SMTP requires a Novell client to work properly with Session Logon.
- **Local Security Policy:** “Log on locally” rights need to be assigned to all domain users. ShareScan requires that the Manager PC login credentials used during normal operation must be those of a local Administrator in order to run the Administration Console. ShareScan Manager cannot be installed on a Domain Controller because of impersonation.

1.2- Support information

This section contains information on the various operating systems, languages, third-party software, and ScanStation PCs supported by ShareScan.

1.2.1 - Languages

ShareScan 5.0 supports the following languages:

- English
- Brazilian Portuguese
- Dutch
- French
- German
- Italian
- Spanish

1.2.2 - Supported devices

For the most current information on supported devices, go to the [Support Web site](#) .

1.3- eCopy connectors

Nuance recommends matching the application credentials (for Lotus Notes, Microsoft Outlook, SMTP, LDAP, and so forth) with the PC login credentials. Nuance recommends creating a generic, email-enabled “ShareScan” account for use by ShareScan.

1.3.1 - eCopy connector for Microsoft Exchange (Mail and/or Fax)

1.3.1.1 - Supported Versions:

- **Microsoft Exchange 2003 / 2007 / 2010**
- For information on supported Microsoft Exchange versions, go to <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.1.2 - Installation Prerequisites And Suggestions

- If configuring the Exchange connector using EWS or WebDAV protocols, the Exchange server SSL certificate must be installed on the PC running ShareScan Manager. Certificates should be installed to the **Trusted Root Certification Authorities** on the Local Computer.
- To configure and use EWS/EWS protocol, the user's logon name and alias must correspond, due to limitations of the Exchange web services. For this reason, using LDAP/EWS protocol is recommended.
- ShareScan 5.0 requires an Outlook client installed on the Manager PC if the connector is communicating with the Exchange server via MAPI protocol. At the time of configuration, the end user should be prepared to provide a user name, password, Exchange server name, and domain name and the general domain environment for a valid Outlook user. Blank passwords and special characters are not supported by ShareScan. To function correctly, **Microsoft Outlook® 2002 / 2003 / 2007 / 2010 (32-bit version)** is required as the client.

1.3.1.3 - Configuring MAPI/MAPI Protocol For Exchange Mail And Fax Connectors

- To configure MAPI/MAPI protocol for Exchange connectors, the service account (the Domain/Username/Password combination) is expecting to have a configured default Outlook profile. Otherwise you cannot configure the connector as the Administration Console will display an error message.
- If your Outlook profile is not preconfigured, you can use the Custom settings via the Administration Console:
 1. Log on to the ShareScan server using credentials of the service account intended for use with the Exchange connectors.
 2. Run the Custom settings of the connector, and enter the email address you want to use. The service account is now ready, and can be used for configuring the connectors.
 3. For Exchange fax connector, define the fax format.
 4. Check to see whether you need to reconfigure your existing profiles using MAPI protocol.
 5. This change does not affect LDAP/MAPI configurations.

1.3.1.4 - Exchange 2010 CAS Support For MAPI Protocol

- To support Exchange 2010 environments that have a dedicated Client Access Server (CAS) separate from the Mailbox Server, a feature was introduced to allow administrators to specify the name of the CAS.
- The relevant property value can be specified either via the **Use CAS** button of the **MAPI** tab in the Administration Console, or in the connector's configuration xml file:
 - For Exchange Mail connector it is [COMMON_APPDATA]\Nuance\ShareScan\connectors\ExchangeMail\Data\ExchangeMailStore.xml

- For Exchange Fax connector it is [COMMON_APPDATA]\Nuance\ShareScan\connectors\ExchangeFax\Data\ExchangeFaxStore.xml

- An example of applying the property value:

```
<?xml version="1.0" encoding="utf-8"?>
<connectorNode>
<Item Key="Groups.AllUsers" Type="Nuance.connectorStore.UserNode">
<UserNode>
...
<Item Key="CasServer" Type="System.String">
<string>EU-Exch-Cas.Nuance.Com</string>
</Item>
</UserNode>
</Item>
```

1.3.2 - eCopy connector for IBM Lotus Notes (Mail and/or Fax)

1.3.2.1 - Supported Versions

- **IBM® Lotus Notes® 8.0 / 8.5**
- **Lotus Domino 7.0 / 8.0 / 8.5**
- For information on supported Lotus Notes versions, go to <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.2.2 - Installation Prerequisites And Suggestions

- The connector requires a Lotus Notes client to be installed on the PC running the ShareScan Manager.
- At the time of configuration, the end user should be prepared to provide an Active ID File, user name, password, and Domino server name.
- When the installer of the Lotus Notes client prompts you to choose between the **Multi-User Install** option and the **Single User Install** option, make sure that you select the **Single User Install** option.

Note:

If **Send messages from personal mail account** is not enabled, all emails will be sent from the user name and password supplied for configuration purposes. Before sending email from a personal Lotus Notes account, the eCopy Mail pass-through database on a Domino HTTP server must be configured. For more detailed information, consult the relevant guide located under **C:\Program Files\Nuance\ShareScan5\Server\LNNotes**.

1.3.3 - eCopy connector for LDAP/SMTP (Mail and/or Fax)

1.3.3.1 - Supported Versions

- **Microsoft LDAP v3**
- **Open LDAP v2.4**

- For information on supported LDAP versions, go to <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.3.2 - Installation Prerequisites And Suggestions

- You will be prompted to enter the following information when configuring the eCopy connector for LDAP: User name, password and IP address, DNS name or URL for the directory being used, search criteria for users and recipients, LDAP Attributes, LDAP port number, and Base DN of the base or root directory in which to search.
- For configuring the eCopy connector for SMTP, you will need to enter the SMTP server IP address or DNS name that will be used for outgoing messages, user name and password, and the SMTP port number.

1.3.4 - eCopy Scan to Desktop

1.3.4.1 - Installation Prerequisites And Suggestions

- Scan to Desktop involves several different components to enable users to scan and send documents to a designated network folder location for modification and storage. A “Scan Inbox” subfolder may be added to existing network home directories or the ShareScan software can create Scan Inbox folder locations. The Inbox Root (Inbox Management directory) stores the user list (`userdirs.txt`) that indicates which users have scan inboxes using Scan to Desktop and whether ShareScan has created Inbox folders; these folders would also reside under this directory.
- For detailed information on configuring Scan to Desktop, see the ShareScan Help, accessible via pressing **F1** on the Administration Console.

Note:

Having the Inbox Root Folder pointing to the existing Network Home Directory Root Folder is NOT supported, as ShareScan modifies the permissions on the root folder.

Inbox Root Directory

The Inbox Root Directory can reside on the ShareScan Services Manager PC or on a network server. If the directory resides locally, it must be configured as a share on an NTFS drive. If the directory resides on a network server, it must be configured as a share on an NTFS drive or on a NetWare drive.

The Inbox Root Directory should not be pointing to a user’s home directory. Choose the Scan to Desktop **Home Directory** option in the connector instead.

Note:

Network home directories configured through a login script are not supported.

ShareScanAdmin Group

An Administrative Group must be used to implement the required security. In previous versions of ShareScan, this group required the name “ShareScanAdmin”. This Administrative Group can now be given any name; however, if multiple Services Managers are pointing to the same `userdirs.txt` file in the Inbox Root Directory, the group to which the service account belongs must be identical on all those Services Managers.

The group used must be created on the domain controller for domain-based networks, on NDS for Novell networks, or on the local machine if the customer is running in a workgroup environment. ShareScan uses this group when assigning permissions to the inbox Root Directory and scan inboxes and requires Full Control. Permissions assigned to the directory are as follows:

Windows (NTFS)

- Administrators – Full Control
- Domain Administrators – Full Control (not used in workgroup configurations) ShareScanAdmin – Full Control
- Inbox Owner – Read or Delete

Novell (Netware)

- Administrators – Full Control
- ShareScanAdmin – Full Control
- Inbox Owner – Read or Delete

An account for an administrative user should also be created and added to the Administrative Group to be used as the Service Account. This user should have a standard user profile with a user name and password. If running in a workgroup environment, a local account should be created for each Scan to Desktop user on the PC where the Inbox location resides.

1.3.5 - eCopy Quick Connect

1.3.5.1 - Supported Versions

- Quick Connect supports Oracle® Database 10g and 11g. When you install Oracle Client 10g/11g, select the Custom Installation option and then make sure that you select the Oracle Provider for OLE DB component. This enables Quick Connect to connect to the Oracle database and store scanned documents and other information.
- Databases: for more information about supported databases, see the eCopy ShareScan 5.0 Software Compatibility Matrix.
- For additional information on supported configurations of eCopy Quick Connect to Database, reference the *Quick Connect Database Recommended Usage* document available for download from eSPN.

1.3.5.2 - Installation Prerequisites And Suggestions

- When selecting a network location as a Quick Connect destination, make sure that the future users have access to the folder or folders being used as storage options. Alternatively, the administrator can use the **Logon As** function to supply login credentials.
- To deliver scanned documents to an Access database, you must disable User Account Control (UAC) on Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2. To disable UAC, type `c:\windows\System32\UserAccountControlSettings.exe` to the command line, and select the appropriate slider setting.

1.3.6 - eCopy connector for OpenText Fax Server (RightFax Edition)

1.3.6.1 - Supported Versions

- For information on supported RightFax versions, go to <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.6.2 - Installation Prerequisites And Suggestions

- The administrator will be prompted to enter a valid RightFax or NT Authentication user name and password. The RightFax server name will also need to be entered.
- The RightFax client software must **NOT** be installed on the system where the ShareScan Manager is installed.
- Delegation privileges, phone books, cover sheets, and billing codes must be configured on the RightFax server in order to be utilized by the eCopy connector for RightFax.

Note:

If "Send from personal account" is not enabled, all faxes will be sent from the user name and password supplied for configuration purposes. NT Authentication functionality requires the Services Manager PC to reside on the same domain as the RightFax server.

1.3.7 - eCopy Scan to Printer

1.3.7.1 - Installation Prerequisites And Suggestions

- In order for a printer to be configured for use with Scan to Print, the appropriate print driver must be installed on the Services Manager PC.

1.3.8 - eCopy connector for Microsoft SharePoint

1.3.8.1 - Supported Versions

- **Microsoft® SharePoint® Portal Server 2003, MOSS 2007, SharePoint Services 2003/2007, SharePoint 2010**
- For more information on supported Microsoft SharePoint versions, see <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.8.2 - Installation Prerequisites And Suggestions

- The administrator should enter a user name and password that will enable the ability to browse to all destination locations, display all index fields, and store documents if "Login As" authentication is used.
- If you are using SharePoint 2003: Microsoft SharePoint Portal Server 2003 or Microsoft Windows SharePoint Servers 2003.
- If you are using SharePoint 2007: Microsoft Office SharePoint Server (MOSS) 2007 or Windows SharePoint 2007 Services.
- If you are using SharePoint 2010: Microsoft SharePoint Server 2010.
- If your company uses a secure SharePoint site, you must install an SSL certification on the ShareScan server.
- Dates are validated by the client regional settings; invalid date formats are not accepted.

- The connector does not fully support storing to workspaces. Storing to an Attendees location is inconsistent and may result in failure to store the scanned document.
- The All Day Event, Recurrence, and Workspace checkboxes will not appear in the calendar list.
- For more information on Microsoft SharePoint, go to <https://www.gosavo.com/ENGAGE> and find the relevant PowerPoint presentation which covers many common connector workflows in ShareScan 5.0.

1.3.9 - eCopy connector for EMC Documentum

1.3.9.1 - Supported Versions

- **EMC® Documentum® 6.0, 6.5, 6.6, 6.7**
- For more information on supported EMC Documentum versions, see <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.9.2 - Installation Prerequisites And Suggestions

- The eCopy connector for EMC Documentum uses the Documentum Foundation Classes (DFC) to connect to the Documentum Server. While all of the necessary DFC files are included with the connector, DFC needs to be configured as part of the installation process.
- For Configuring DFC the following information is required:
 - The Primary *Connection Broker* Host Name: Broker Server Name
 - Port number: Default = 1489
 - Repository Name
 - Login Name and Password to that Repository
 - The DFC should be in the same domain as Documentum server
- The eCopy connector for EMC Documentum will then need the Repository chosen from the drop-down menu, as well as a user name and password. In the connector Administration, all Repositories available through that Connection Broker will now be available. The administrator should then enter a user name and password that enables browsing to all desired destination locations within the selected repository and store documents if "Login As" authentication is used.
- If you are using a firewall, you must add `SQLSERVER.exe` and UDP port 1434 to the exceptions list.
- It is strongly recommended that you store documents using the doctype named "dm_document" or a customized doctype that is based on "dm_document".

Notes:

- **Connection Broker** – Named DocBroker in previous versions of Documentum. Connection Broker is a service that runs on a Documentum server; it is a connection point from the client.
 - **Repository** - Named Docbase in previous versions of Documentum. It is a document database on the Documentum server. The Connection Broker establishes the connection between the connector and the Repository.
-

1.3.10 - eCopy connector for Autonomy iManage WorkSite

1.3.10.1 - Supported Versions

- **Autonomy (Interwoven) iManage (WorkSite) 8.0, 8.2, 8.4, 8.5**
- For more information on supported Worksite versions, see <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.10.2 - Installation Prerequisites And Suggestions

- The administrator should enter a user name and password that enables browsing to all destination locations, display all index fields, and store documents if **Login As** authentication is used.
- For more information on Impersonation passwords, the administrator should refer to the WorkSite documentation. Note that Impersonation is only available when using Trusted Login and authenticating against Novell.
- When you use Novell Trusted Login, make sure that the Novell Client configuration on the computer running the ShareScan Manager includes a value for the **Preferred Server** option. If you leave this field blank or you enter an incorrect value, users will not be able to store scanned documents.
- For more information on Worksite, go to <https://www.gosavo.com/ENGAGE> and find the relevant PowerPoint presentation which covers many common connector workflows in ShareScan 5.0.

1.3.11 - eCopy connector for Open Text Content Server - eDOCS Edition

1.3.11.1 - Supported Versions

- **Open Text Document Management, eDOCS Edition/(Hummingbird) 5.1.05, 5.2, 5.3 and 5.3 SP2, 6.0.5**
- For more information on supported eDOCS versions, see <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.11.2 - Installation Prerequisites And Suggestions

- Before installing the connector, the Administrator must install the Windows Explorer DM Extension software for Livelink ECM - eDOCS DM on the eCopy ShareScan Services Manager PC. Then run the DM Connection Wizard. Both versions of the DM Extension software include the required DM API and the DM Connection Wizard.
- Install the Windows Explorer DM Extension component only (under "Optional Components").
- You must select "Intranet Mode" (the default mode). Do not select "Internet Mode".
- After installation, launch the DM Connection Wizard and enter the name of your DM server.
- The eCopy ShareScan Services Manager must be on the same domain as the DM server, for the DM Connection Wizard to establish a connection with the server.
- The Administrator will need to enter a valid eDOCS DM user name and password that has the ability to store documents if "Login As" authentication is used.
- Nuance Communications recommends that you add the eCopy Document Type and Application ID to your eDOCS (Hummingbird) server. See your server documentation for details.

- When the eDOCS DM Extension Client v 5.1.0.5 SR6 or later is installed on the same computer as the ShareScan Manager (not in the same domain as the DM server), you cannot configure the eCopy connector.
- Default values that are assigned by the eDOCS DM server appear in the Client. To use a different value, you must remove the default value and then use the Search feature or the "Search while typing" option to specify the new value.
- If a profile for an application does not appear, contact your administrator. The application may be disabled from within the eDOCS DM software.
- Before installing the eCopy connector for Open Text Content Server, the Administrator must install and configure the Windows Explorer DM Extension software for Open Text Document Management, eDOCS Edition 5.1, 5.2, 6.0 or later or Hummingbird DM 5.1, 5.2, and 6.0 on the same PC as the eCopyShareScan Manager. After that, run the DM Connection Wizard.
- Both versions of the DM Extension software include the required DM API and the DM Connection Wizard.
- For instructions about installing the DM Extension software, refer to your eDOCS documentation.

1.3.12 - eCopy connector for Open Text Content Server

1.3.12.1 - Supported Versions

- **Open Text Content Server 9.2, 9.5, 9.6, 9.7, 10.0**
- For more information on supported Open Text Content Server versions, see <https://www.gosavo.com/ENGAGE> and search for ShareScan 5.0 Compatibility Matrix.

1.3.12.2 - Installation Prerequisites And Suggestions

- The administrator should enter a user name and password that enables browsing to all destination locations, display all index fields, and store documents if "Login As" authentication is used.
- The eCopy connector for Livelink ECM uses the Livelink API (LAPI) and supports TCP/IP direct connections with native Livelink authentication. It does not support HTTP or HTTPS connections or non-native authentication methods. Native authentication using LAPI supports Livelink authentication, NTLM authentication, and LDAP authentication. The Livelink server is responsible for managing the authentication settings and the connector works transparently with the selected authentication mode.
- If the Open Text Content Server environment requires a user to change password at the next logon to the system, the user must change the password at the workstation before using ShareScan. If the user does not do this, the system will display a message that the password has expired and that the user will not be able to store the scanned documents.
- For authentication methods outside of these constraints, refer to your eCopy Technical Consultant.
- The Administrator will need to provide the following information to properly configure the connector:
 - Livelink Database name.
 - Livelink Server name.

Note:

The server entered in the "Livelink Server" field must be on the same network (LAN) or connected via a VPN (WAN) as the Services Manager. It cannot be a web-only connected server. The Livelink connector does not communicate over

HTTP or HTTPS; instead it uses TCP/IP and LAPI over the specified port. Even if port 80 is entered in the port field, it will not force the connector to communicate over HTTP or HTTPS.

- Port - This is the port that the LiveLink Server is communicating on. The default is 2099.
 - Username and Password - This is a user account that the connector uses to test the connection and get a list of usernames to display to the user for selection.
-

Note:

The Livelink Database information can be found on the Livelink Administrative Site under the *Database Administration* section.

- For more information on eCopy connectors, go to <https://www.gosavo.com/ENGAGE> and find the relevant PowerPoint presentation which covers many common connector workflows in ShareScan 5.0.

2 - Installing ShareScan

The following chapter contains information on the various tasks associated with installing ShareScan.

2.1- Basic workflow

To install, configure, and license ShareScan:

1. Install the ShareScan software on a network computer. You have the option to customize the database installation. For more information, see the **Custom database installation options** chapter of this guide.
2. Install ShareScan Client, if needed (for more information on installing the client, see the **Client-side installation** chapter of this guide).
3. Start the Administration Console.
4. Add licenses, add devices (if they do not appear automatically on the **Devices** tab), and/or set up scanners.
5. Install and configure Services, Connectors, and Devices.

When you open the Administration Console, the **Welcome** page displays a list of the main tasks that you can perform, in the recommended configuration sequence: Services, Connectors, and Devices.

For in-depth information about configuring and managing the Services, Connectors, and Devices that ShareScan uses, refer to the ShareScan Help. To access the Help, click **F1** or click the **Help** button that is located in the upper-right corner of the ShareScan Administration Console.

2.2- Installing ShareScan

Use the ShareScan installation program to install the software components on a network computer.

Notes:

When running Windows Vista, Windows 7, Windows Server 2008 R2 or Windows Server 2008, ensure that the .NET Framework core feature is set to **Enabled**. You can do this via **Control Panel > Turn Windows features on and off**. ShareScan is only compatible with the Apache Tomcat version included in the installation program. If you have Apache

Tomcat already installed, remove it prior to installing ShareScan.

If you have Skype installed, it can conflict with the Apache Tomcat installed by ShareScan. To avoid this, ensure that the **Use port 80 and 443 as alternatives for incoming connections** option is unchecked in Skype.

Ports to be left open

Ensure that the following ports are left open:

- TCP: 80, 8080, 443, 9030, 9100, 9600, 9601, 9200-9220, 50001, 50002, 2121, 8009, 8005
- UDP: 8125, 161, 9988, 8899

To install the software:

1. Ensure that you have the latest system updates on your machine and that Automatic Windows Updates are turned off.
2. Insert the ShareScan installation medium in the drive.
3. Run **setup.exe**.
4. Choose a language for your installation.
5. Click **Start Installation**. The InstallShield Wizard displays a screen that identifies the software prerequisites for your computer.
6. Click **Install** to install the required software.
Installation of the Microsoft.NET Framework takes a little while and requires a restart of the computer. After you restart the computer, you can proceed with the rest of the installation.
7. When installation of the required software is complete, the **Welcome** page for the installation appears. Click **Next**.
8. When the **Customer Information** window opens, enter a valid license key.
9. Click **Next**. You have to accept the License Agreement to proceed to the **Destination Folder** window.
10. Accept the default installation folder (recommended) or select a different folder and then click **Next**.
11. Select the program features you want to install on the **Custom Setup** window. The InstallShield Wizard offers you a number of customization options. For a detailed description of the options, see **Custom database installation options** below.
 - When selecting **Complete Install**, SQL Server 2008 R2 Express is installed and a ShareScan database is created.
 - When selecting **Custom Install**, you can customize which components are installed. Apart from the ShareScan Server itself, you can install an SQL Server and a ShareScan database. If you decide to use a different instance and/or database, you have to provide the relevant data (for example, server name, IP address, and so on) for the installer. To select an existing SQL Server, it is recommended that you use the **Browsing** option.
 - You must connect to a ShareScan database. ShareScan uses SQL server authentication to connect to databases. If you install only the ShareScan database, the **Add / Remove Programs** list of the **Control Panel** will show ShareScan as installed. You have to remove that entry first if you want to install the product at a later point.

12. Click **Next**. The **Ready to Install the Program** window opens.
13. Click **Install**.
14. When the installation is complete, click **Finish**.

If you want to launch the Administration Console immediately, select the checkbox.

You are now ready to configure a connector profile.

2.2.1 - Custom database installation options

If you deselected either the ShareScan database feature or Microsoft SQL Server Express 2008 R2 (or both), you must provide proper credentials to an existing SQL server using SQL server authentication. You can prevent several issues by using the **Browse** button and allowing the installer to search for available SQL servers on the network instead of typing the name of the favored SQL server. Click **Next** and the installer validates the provided credentials and notifies you of any errors encountered.

2.2.1.1 - No SQL Is Installed

1. Deselect the Microsoft SQL Server Express 2008 R2 feature
2. Specify where you want to create the ShareScan database.
This can happen either on local or remote SQL servers, where the specified credentials are sufficient and the SQL server version is not older than Microsoft SQL Server 2005 with latest service packs.

2.2.1.2 - Only ShareScan Is Installed

1. Deselect both database-related features. Only eCopy ShareScan 5.0 is installed on the target machine.
2. The installer asks for credentials for any available SQL server where a ShareScan database is available.
3. If you provide credentials to an SQL server where no ShareScan database is installed, the application does not function and you have to create the database manually with the provided tools and scripts in the fileset.

2.2.1.3 - Only The ShareScan Database And The SQL Server Are Installed

1. Deselect only the eCopy ShareScan 5.0 feature
2. The SQL server is installed locally and a ShareScan database is created by the installed server. If you want to install eCopy ShareScan 5.0 on that machine later, you must remove the “eCopy ShareScan 5.0” entry from **Add/Remove Programs** and rerun the installer with a different Custom Setup case.

Alternatively, you can install only the ShareScan Database to either a local or a remote SQL server.

2.3- Adding devices

After adding a license file to the ShareScan system, you add one or more embedded or integrated devices.

Note:

For instructions about removing devices, refer to the ShareScan Help.

To add a device to the Manager:

1. Make sure that the device you want to add is running, and is not in sleep/energy save mode.
2. In the Administration Console, on the Ribbon, click **Add Device**. You can also select **Devices** on the **Welcome** page and then right-click in the **Device Configuration** pane and select **Add Device**. The **Add Devices** window opens. The window displays available eCopy-enabled devices along with information such as the host name, the IP Address, the vendor, Client software version, and the Manager that is currently managing the device.
3. If a device that you want to add does not appear in the list of available devices, select a protocol in the **Discovery** list and then click **Refresh**.
4. Select the device or devices that you want to add and then click **OK**.
5. When the system prompts you to confirm the device that you want to add to the device list, click **OK**.

Troubleshooting tip: If your device(s) cannot be discovered and are not shown in the list on the **Add device** dialog with any of the protocols, then make sure that:

- The device is up and running.
- It is connected to the network (use the `ping <IP-address>` command in a command window).
- In case of non-web based devices, the ShareScan client software is installed and enabled (running).
- The required ports are open on the firewalls/routers.

Note:

The automatic device discovery is only supported via UDP. If the autodiscovery does not succeed, use TCP/IP to add the device manually.

2.4- Upgrading ShareScan

This section contains information on upgrading your existing ShareScan installation.

2.4.1 - Upgrading from ShareScan 4.x

If you have ShareScan 4.x on your system, the installer will perform an upgrade to the latest software.

Note:

Upgrading from 3.x versions is not supported.

To upgrade the software:

1. In the **Launch** window, click **Start Installation**.
2. Click the **Upgrade** option.
The upgrade process starts. The preparatory phases include backing up existing ShareScan data (services, connectors, and devices) and uninstalling the existing ShareScan software, services, connectors, and devices.
3. Once the above tasks are completed, the ShareScan installation commences.

Note:

Nuance recommends that you back up the connector configuration and license data prior to upgrading ShareScan.

2.4.2 - Upgrading ShareScan 5 with Service Packs

If you are upgrading from an existing version of ShareScan 5

1. Close the Administration Console.
2. Run the Service Pack executable.

Service Packs do not require the previous Service Pack to be present on your machine.

3 - Client-side installation

The following chapter contains information on installing device-specific embedded clients and ScanStation drivers.

3.1- Installing the ShareScan Ricoh client

This section contains information on installing the ShareScan Ricoh client.

ShareScan supports the following devices:

- v4, v5, v6, and v7 devices running the latest SDK/J version

The ShareScan Ricoh client is available in two Zip files:

- ClientWEBv2v4_<jar_version>.zip
- ClientSDv2v4_<jar_version>.zip

Depending on the installation method, you need one of these files.

This section describes three installation methods:

- Install the Ricoh client via the Administration Console
- Use the Ricoh Web Image Monitor to install the ShareScan Ricoh client, using ClientWEBv2v4_<jar_version>.zip. For more instructions, consult your Web Image Monitor manual.
- Install the Client from an SD card that you create, using ClientSDv2v4_<jar_version>.zip

These procedures assume that the proper firmware and SDK/J version is installed on the device.

The Ricoh client offers the following additional configuration option, available via the ShareScan Administration Console:

- **Suppress Preview and Settings:** enabling this setting reduces time spent at the device. Suppressed visuals are available to the user on-demand.

3.1.1 - Installing the ShareScan Ricoh client without remote installation

On a number of Ricoh devices, remote installation via the Add Device Wizard is not available, thus you have to install the JAR file manually. To do so, follow the instructions below.

Note:

You need administrator rights to perform the operations. The necessary registry files are downloadable from [AskeCopy](#).

The MFP models that require this type of installation are as follows:

- Aficio MP 2352 Series
- Aficio MP 2852 Series
- Aficio MP 3352 Series
- Aficio SP 5200S
- Aficio SP 5210SF
- Aficio SP 5210SR

If you have a mixed fleet comprising of MFPs from these device families, and older devices (in any combination), then first add the older devices via the usual methods (via Administration Console, SD card or web browser, as detailed in the relevant chapters), then perform the steps outlined in this chapter for Aficio devices mentioned above.

3.1.1.1 - For 32-bit Systems

1. Run `RicohLatestModelsSupportMode_ON_32bit.reg` to enable support for the listed devices.
2. Install the JAR file to the device via SD card or Web Image Monitor (for more information, see the relevant chapters of the installation guide).
3. Restart the ShareScan Manager.
4. Via the ShareScan Administration Console, simply click through the **Add Device** procedure.
5. Run `RicohLatestModelsSupportMode_OFF_32bit.reg` to finalize the installation.

3.1.1.2 - For 64-bit Systems:

1. Run `RicohLatestModelsSupportMode_ON_64bit.reg` to enable support for the listed devices.
2. Install the JAR file to the device via SD card or Web Image Monitor (for more information, see the relevant chapters of the installation guide).
3. Restart the ShareScan Manager.
4. Via the ShareScan Administration Console, simply click through the **Add Device** procedure.
5. Run `RicohLatestModelsSupportMode_OFF_64bit.reg` to finalize the installation.

3.1.2 - Installing the ShareScan Ricoh client via the ShareScan Administration Console (recommended)

1. Ensure that the Ricoh device is running.
2. Ensure that the ShareScan Administration Console is running.
3. Download the ShareScan Ricoh client (`ClientWEBv2v4_<jar_version>.zip`).
4. Either right-click **Device configuration** and select the **Add device** menu item or click **Add device** on the ribbon bar.
5. The **Add devices** window opens, displaying the available devices.
6. If a device that you want to add does not appear in the list of available devices, choose from a drop-down list in Discovery, select a protocol, and click **Refresh**. Select the device and click **OK**.
7. The Add Device dialog displays the device's IP address. Click **Next**.

8. The following dialog allows you to install a new, or upgrade an existing ShareScan Ricoh client on this device. Click **Browse** and locate the `ClientWEBv2v4_<jar_version>.zip` file.
9. If you are installing the ShareScan Ricoh client on the device for the first time (no previous ShareScan Ricoh client is installed on the device), click **Finish**.
10. If you are upgrading a previous version of the ShareScan Ricoh client (already installed on the device), click **Install**. The text area below displays steps in the upgrade process, including:
 1. stopping the ShareScan Ricoh client,
 2. uninstalling the ShareScan Ricoh client
 3. rebooting the device
 4. installing the new ShareScan Ricoh client, and
 5. starting the ShareScan Ricoh client.

3.1.3 - To install the ShareScan Ricoh client via a Web browser:

1. Make sure that the Ricoh device is running.
2. Open a Web browser and then connect to the device by entering the IP address of the device in the address bar of Internet Explorer, as in the following example: *http://10.10.12.99*.

The **Web Image Monitor** page opens, displaying information about the device.

3. To log in to the device:
 - Click the **Login** button, which is in the upper-right corner of the page.
 - Enter the device administrator credentials in the **Login User Name** and **Password** fields.
 - Click **Login**.
 - The **Administrator** page opens, enabling you to configure the device.
4. In the navigation pane, click **Configuration** and then scroll down to the **Extended Feature Settings** area.
5. Click **Extended Feature Info**.

The **Extended Feature Info** page displays information about the version of the Java™ platform and identifies the slot in which it is installed. Click **Back** to return to the **Extended Feature Settings** area.

6. To install the ShareScan Client:
 - In the **Install** area, select **Local File** and then click **Browse**.
 - Navigate to the location of the `ClientWEBv2v4_<jar_version>.zip` file.
 - In the **Choose file** window, select the `ClientWEBv2v4_<jar_version>.zip` file and then click **Open**.
 - Click **Display Extended Feature List**.

The **Display Extended Feature List** page opens.
 - Under **Installation Target Setting**, select **Install to Device HDD** and then set **Auto Start** to **On**.
 - Select the **ShareScan Xlet** and then click **Install**.
 - Review the information on the confirmation page, making sure that the startup location is “Device HDD” and then click **OK** to start the installation.

When the installation is complete, the **Configuration** page opens.

7. To start the application:

- When the **Configuration** page opens, scroll down to the **Extended Feature Settings** area.
- Click **Extended Feature Info** to verify installation of the application and then click **Back**.
- Under **Extended Feature Settings**, click **Startup Setting**, make sure that the ShareScan application is selected, and then click the **Startup/Stop** button.

The status of the application will change to “Starting Up”.

8. To log out of the Web Image Monitor, click the **Logout** button in the upper-right corner of the page.

3.1.4 - To install the ShareScan Ricoh client from an SD card:

1. To create an SD card:

- Locate the downloaded `ClientSDv2v4_<jar_version>.zip` file.
- Extract all the files from the `zip` file to the following location on the SD card (retaining the folder structure is important):

```
sdk\dsdk\dist\33952001
```

2. If you are not the person who installed the SDK/J and you do not know which slot the SDK/J SD card is installed in, press the **User Tools/Counter** button on the device panel. Then, on the display panel, press **Extended Feature Settings > Extended Features**. Note the SD Card Slot number for the Java™ platform and then press **Exit** twice.

3. Turn off the main power switch. If necessary, see the documentation for your device for the location of the main power switch.

When the power is off, the Main Power indicator on the control panel, located above the On indicator for the Operation switch, will no longer be illuminated.

4. Insert the SD card in the slot that does not contain the SDK/J SD card and then turn on the main power switch..

The Main Power indicator will be illuminated.

5. Press **User Tools/Counter**.

6. Press **Extended Feature Settings**.

7. Press **Extended Feature Settings** again.

8. To install the ShareScan Client:

- Press the **Install** tab and then select **SD Card**.
- Select the **ShareScan Xlet**.
- Select **Machine HDD** as the installation target and then press **Next**.
- When the **Extended Feature Settings** screen appears, press **OK**.

Note:

Nuance recommends that you leave the Auto Start option selected during installation.

- When the installation is complete, press **Exit**.

9. Turn off the main power switch and then remove the SD card.
10. Turn on the main power switch.

With the **Auto Start** option selected, the application will start when the device is started up.

3.1.5 - To uninstall the ShareScan Ricoh client via a Web browser:

1. Make sure that the Ricoh device is running.
2. Open a Web browser and then connect to the device by entering the IP address of the device in the address bar of Internet Explorer, as in the following example: *http://10.10.12.99*.

The **Web Image Monitor** page opens, displaying information about the device.

3. To log in to the device:
 - Click the **Login** button, which is in the upper-right corner of the page.
 - Enter the device administrator credentials into the **Login User Name** and **Password** fields
 - Click **Login**.

The **Administrator** page opens, enabling you to configure the device.

4. In the navigation pane, click **Configuration** and then scroll down to the **Extended Feature Settings** area.

Click **Extended Feature Info**.

The **Extended Feature Info** page displays information about the installed application. Click **Back** to return to the **Extended Feature Settings** area.

5. To uninstall the ShareScan Client:
 - In the **Uninstall** area, select the **ShareScan** application.
 - Click **Uninstall**.
 - Review the information on the confirmation page and then click **OK** to start uninstalling the application. Respond to any warning messages.

When the process is complete, the **Uninstall** page opens. The application no longer appears in the list of applications.

6. Turn off the main power switch.
7. Turn on the main power switch.
8. See the instructions for installing the Client.
6. To log out of the Web Image Monitor, click the **Logout** button in the upper-right corner of the page.

3.1.6 - To uninstall the ShareScan Ricoh client from a device:

1. Press **User Tools/Counter**.
2. Press **Extended Feature Settings**.
3. Press **Extended Feature Settings** again.
4. To stop the application, select **Startup Setting** and then select **ShareScan**.

You may have to do this twice. The status must be "Stop".

5. To uninstall the Client, select the **Uninstall** tab, select **ShareScan**, and then press **Yes**.

The **Complete extended feature uninstallation** window opens.

6. Press **Exit**.

The **Ready to uninstall** window opens.

7. Press **Exit**.

8. Turn off the main power switch.

9. Turn on the main power switch.

3.2- Installing a Ricoh ScanStation Driver

This section contains information on installing the Ricoh ScanStation driver.

The ScanStation uses a driver to get input from the device. You must install and configure the driver before licensing the device.

To ease your device configuration task, some settings may be disabled in the Scanner Setup Wizard.

Version 4.0 Ricoh TWAIN drivers include a Network Connection Tool. When you have multiple devices of the same model type, you use the tool to select the specific device on your network that you want to use with the driver. If you are using a version 3.0 Ricoh TWAIN driver, your system will automatically connect to the first device it finds on your network that uses the driver.

To install the driver

1. Download the driver from the Internet.
2. Run the installation program, following the instructions on the screen.
3. When the installation is complete, click **Finish**.

To configure the driver

1. Select **Start > Programs > <driver_name> > Network Connection Tool**.
2. Select the **Use a specific scanner** check box.
3. Click **Search Scanner**.

The **Search Scanner: Result** window lists all devices on the network that can use the current TWAIN driver.

4. Select the scanner that you want to use and then click **OK**.

The **Network Connection Tool** window opens.

5. Click **OK**.

3.2.1 - ISIS drivers

In addition to scanning via TWAIN, ScanStation also supports ISIS-scanning. Install the ISIS driver supplied by the manufacturer of the device, then use the Scanner Setup Wizard to configure its use with ScanStation.

If any scanning issue occurs with ScanStation, please test first whether you are able to scan into another ISIS supported application.

4 - Licensing devices

Every device that you use with Nuance Communications software requires a valid license. ShareScan 5.0 uses a digitally signed license file, which contains a unique license key generated by Manufacturing. The license key is a unique ID that is associated with the hardware ID (HID) of the PC where the ShareScan database is installed.

Note:

ShareScan 5.0 licensing is different from ShareScan 4.x licensing, which was based on the association of a product key with a device. Licensing is no longer associated with a particular device, but the HID of the SQL server.

Site licenses, valid for activation with a predefined number of devices, are also available. After a license file is created for the specified number of devices, it cannot be modified to increase the number of devices; if you purchase additional devices, you need to purchase additional license(s), and those license(s) will be delivered as separate license files. When you load the new license file, the Administration Console can merge the original license file with the new file.

After adding a license, you can add one or more embedded or integrated devices to the Manager. (You can add these devices at any time. However, if you add them before activating the license, a 30-day grace period starts for the license.)

For ScanStation systems, the local device is automatically added; then, when the administrator selects the driver, the system verifies the validity of the license file.

ShareScan 5 includes a Licensing Wizard, which handles the following license-related tasks:

- loading licenses,
- activating licenses,
- loading activated licenses,
- reactivating licenses,
- removing licenses.

4.1- Loading licenses

You can use the automatic license download function, or import the license file(s). If no internet connection can be detected, only the second option is available.

1. Click the **Load license** button of the License Wizard. The Welcome screen is displayed.
2. Click **Next** to continue.
3. Select **Download license automatically** when specifying the source. The **Automatic license download** screen is displayed.
4. Copy the license keys of the licenses to download in the text box. Click **Add** after each. When the list below is complete, click **Next**. The **Select license files to load** screen is displayed.
5. Click the **Browse** button to add new files to the list of files to be imported. When finished, click **Start import**.
6. Click **Start** to begin loading licenses.
7. Click **Finish** to close the License Wizard.

4.2- Activating licenses

You need to activate a license only once; thereafter, it is associated with the PC where the ShareScan database is installed.

1. Click the **Activate** button of the License Wizard. The Welcome screen is displayed.
2. Click **Next** to continue.
3. Specify the hardware ID. Click **Next** to continue.
4. Select **Automatic activation** on the **Select activation mode** screen.
5. Click **Next** to continue. The **Output file creation / Activation** screen is displayed.
6. Click **Start** to begin activation. The **Specify file output** screen is displayed.
7. Click **Next** to continue.
8. Click **Finish** to close the License Wizard.

4.3- Loading activated licenses

Use this option when importing already activated licenses to ShareScan.

1. Click the **Load activated** button of the License Wizard. The Welcome screen is displayed.
2. Click **Next** to continue. The **Select license files to load** screen is displayed.
3. Click the **Browse** button to add new files to the list of files to be imported, When finished, click **Start import**.
4. Click **Start** to begin loading licenses.
5. Click **Finish** to close the License Wizard.

4.4- Reactivating licenses

Reactivation is necessary when the hardware running the database server is replaced. Prior to reactivation, you must remove the licenses (see **Removing licenses**, below).

1. Click the **Reactivate** button of the License Wizard. The Welcome screen is displayed.
2. Click **Next** to continue.
3. Specify the hardware ID.
4. Click **Next** to continue. The **Specify file output** screen is displayed.
5. Enter the output file name and the path of the collected licenses.
6. Click **Next** to continue. The **Output file creation** screen is displayed.
7. Click **Start** to create the output file.
8. Click **Finish** to close the License Wizard.

4.5- Removing licenses

Use this option when transferring licenses from the current ShareScan installation. After the removal is complete, the licenses can be safely transferred and reactivated.

1. Click the **Remove** button of the License Wizard. The Welcome screen is displayed.
2. Click **Next** to continue. The **Select licenses** screen is displayed.
3. Select the license(s) you want to remove, then click **Next**.
4. Click **Start** to remove the selected license(s).
5. Click **Finish** to close the License Wizard.

5 - ShareScan post-install

Now that you have completed the basic installation, configuration, and licensing steps, you are ready to perform other tasks, including:

- Configuring system settings.
- Installing and configuring additional connectors, services, and extenders.
- Licensing additional devices and monitoring activity between devices and the Manager.
- Accessing and configuring other Managers.
- Configuring, backing up, and restoring the ShareScan database.

5.1- ScanStation post-install

The ScanStation device automatically appears on the **Devices** tab. Test your configuration either by using the built-in Simulator, or by verifying the configuration at the device.

After installation, configure the following options:

- **Configuration:** If **Show Title Bar** is not checked, the client runs in kiosk mode. You can use the Password (exit) option for clients in kiosk mode to set up a password that is required to exit the ScanStation client.
- **Scanner Defaults:** Configure according to the device you are using. For more information, refer to the Administration Console Help.
- **ScanStation Startup Configuration:** Configure the options for the ScanStation client startup.

5.2- Send to eCopy service

The Send to eCopy[®] service is a ScanStation extension that is installed to ease the interworking of non-TWAIN, non-ISIS scanners and ShareScan.

The service allows you to configure a local folder or network shared folder on the ScanStation machine, which is used by Send to eCopy as a source folder, from where it picks up images for processing.

To use the service, the scanner must be configured to have access to the watched folder. Also, the administrators of the Send to eCopy service must supply an instruction image, which contains guidelines for the scanning procedure, and is displayed at the ScanStation screen when accessing the Send to eCopy service.

The functionality supports the following file types:

- Single-page: .bmp, .jpeg, and .tif
- Multi-page: .tif, .pdf

To use the functionality, the “replaced” device must be able and configured to produce files in the above formats.

5.2.1 - Send to eCopy configuration options

The service is available via the **Scanners** tab of the **Settings** pane in the Administration Console. To use Send to eCopy, ensure that you have selected the ScanStation workstation as the device.

5.2.1.1 - Configuration Settings:

- **Driver name:** here you can select the scanner which is “replaced” by the Send to eCopy service.
- **Show Title Bar:** checking this option allows you to set whether the ScanStation title bar is visible. If the title bar is not visible, the ScanStation application runs in Kiosk mode.
- **Password (exit):** The password that must be typed to exit the application when it runs in Kiosk mode.

5.2.1.2 - Send To ECopy ShareScan Settings

- **Instructions Image:** the location of the instruction image. While Nuance supplies a default image, Send to eCopy users should modify this image depending on the scanner models and the actual UI language they use with the service.
- **Watch Folder:** this is the local folder or network shared folder that the service is watching for scanned documents.
- **Filter:** here, you can select which types of image files you wish to see. Other files are ignored by the Send to eCopy service.
- **Inactivity Timeout:** here you can set the timeout value (in milliseconds) for the communication between the scanner and the Send to eCopy service. If the images have arrived and the application does not pick them within this timespan, the Send to eCopy service deletes them.
- **Session Timeout:** here you can set the timeout value (in milliseconds) for the communication between the ScanStation application and the Send to eCopy service. At the beginning of each scanning session, the application opens a session and receives a new session ID from the Send to eCopy service. After that, the application uses this session in all subsequent Send to eCopy service calls. If there is no call from the application to the Send to eCopy service within the timeframe specified here, the service considers that the application stopped working and terminates the session. This also means that any remaining images are deleted.
- **First Page Timeout:** this value controls how long the ScanStation application waits for the first page of the scan job to arrive from the Send to eCopy service. The value is given in milliseconds.
- **Next Page Timeout:** this value controls how long the ScanStation application waits between receiving the additional pages of the scan job. The value is given in milliseconds.

- **Use Lock File:** set this option to **True** to prevent different Nuance applications from monitoring the same folder. The service uses a lock mechanism which is used by other Nuance applications as well, so it can detect if another Nuance application is already monitoring the specified watch folder.
- **Use Encryption:** setting this option to **True** means that documents in the watched folder are encrypted while waiting for the service passing them to ScanStation. Because of Windows security settings, encryption works for local watch folders only.
- **Domain / User Name / Password:** the credentials of the domain containing the watched folder (if it is a network folder).

5.3- Configuring ShareScan (examples)

This section outlines the basic process to

- Configure a service (Activity Tracking)
- Configure an Extender (Forms Processing Extender)
- Configure a connector profile (QuickConnect) using the already configured service and extender
- Test your saved profile in the built-in simulator

When a user presses a connector button, the connector uses the settings specified in the connector profile that is associated with the button, such as the button label and image, encryption of scanned documents, and the services to use with the connector.

The recommended workflow is to configure services and extenders first, so that they are available when you configure a connector profile, and then configure connector profiles.

You have the option to set up any connector with the **Bypass redirect screen** option. Using this option navigates the user back to the Main Form at the end of the session or logout automatically if **Session Logon** is enabled.

The procedure in this section provides you with enough information to complete the basic configuration process. For in-depth information, refer to the ShareScan Help.

5.3.1 - To configure a service (example – Activity Tracking):

1. Start the ShareScan Administration Console by clicking **Start > Programs > eCopy Applications > ShareScan 5.0 > ShareScan Administration Console**.
The system initializes the .NET framework, retrieves configuration information from the ShareScan database, and then displays the ShareScan Administration Console.
2. Select the **Services** tab.
The **Configure Services** pane displays a list of the installed services, including connector services, device services, and common services.
3. In the **Device Services** list, select **Activity Tracking**. The **Configure Activity Tracking Service** pane opens.
4. Select **Yes** for the **Configured** setting and then click **Save**. For more information about configuring the Activity Tracking service, search for the "Activity Tracking service" topic in the Help.

5.3.2 - To configure an Extender (example – Forms Processing Extender):

In this example, this Extender is used to process scanned forms, extract form data, and make it available for Quick Connect via data publishing (using batching).

1. Download the Forms Processing Extender package.
2. Open its configuration guide and proceed with the installation.
3. When you have finished the installation, reboot your machine, then configure the Extender. Then create a template library, and a template. Make sure your template contains at least one uniquely named zone from which content can be passed to Quick Connect.
4. Test your template.
5. After you have finished designing and testing your template, make sure you enable batching in the Extender by marking the **Batch on Matched Templates** checkbox.
6. Save your configuration.

5.3.3 - To configure a Quick Connect connector profile to use Forms Processing Extender data

1. Select the **Connectors** tab.
The **Configure Connectors** pane displays a list of the available connectors.
2. Select QuickConnect.
3. The **Configure Connector (Quick Connect)** pane and the **Settings** pane open.
4. Select the **Destinations** tab, then click **New**. Name the destination, set its **Type**, **Location** and specify **Authentication** options.
5. Select the **File name** tab, and set the file naming convention for the connector.
6. Optionally, select the **Index file** tab, and set the index file attributes.
7. Use the **Settings** pane to configure the following:
 - display settings,
 - document settings,
 - service to be associated,
 - extender to be associated,
 - scanner settings, and
 - offline processing settings.
8. Click the **Save Current Profile** button. For more information about configuring the settings for a connector, open the relevant Help topic.

5.3.4 - To test the configuration of a profile:

1. In the Administration Console, select the **Devices** tab.
The **Device Configuration** pane displays the simulator and any installed devices.
2. Select the device simulator.
The **Configure Connectors for Device - Simulator** pane lists the available profiles.
3. In the **Select Profile(s)** column, select the profile that you created for the Quick Connect connector, and then click **Save**.

4. On the **Ribbon**, click the **Simulator** button. The simulated Client screen displays the button for the connector you configured.
5. Click the Quick Connect icon on the simulated client screen. The **Preview** screen is displayed.
6. Click **Next** to continue. The Forms Processing Extender screen is displayed.
7. Check the field values, then click **Next** to continue.
8. Select a **Destination**, then click **Send** to continue.
9. Select the post-processing option you want to use.

6 - Next steps

After finishing the basic installation and configuration tasks, you can start using and customising ShareScan via the Administration Console.

The ShareScan 5.0 user interface is organized differently from the user interface in previous versions of the product. In the new Administration Console, all system functions are available on the Ribbon and there are separate tabs for configuring services, connectors, and devices.

System functions are available on the **Home** tab and the **Advanced** tab. The **Home** tab contains the most frequently used functions, such as managing the ShareScan Manager; the **Advanced** tab contains less frequently used functions and several new functions, such as managing the ShareScan database.

When you open the Administration Console, the **Welcome** page lists the main functions in the recommended order for performing each function:

- Configure one or more installed services, so that they will be available when you configure connectors and devices. There are three types of services: services that you apply to a connector, services that you apply to devices or device groups, and services that you apply to connectors and devices.
- Configure one or more profiles for the installed connectors that will be used on the scanning devices. You can create multiple profiles for each connector and you can activate each connector profile on multiple devices.
- Register ShareScan online.

When you click the Services, Connectors, or Devices links, a pane lists the items that you can configure. After you select an item, such as Session Logon, ShareScan opens one or more panes where you specify the appropriate settings.

6.1- Best practices

Ensure that the %temp% environment variable is set.

Ensure that all critical automatic updates are applied to target systems and that automatic updates are turned off for the time of installation.

Do not wait too long to click the **Install** button; otherwise, the increased storage usage in the temp folder can trigger a cleanup process that causes installation failure.

After installation you may check to see whether the following services are running:

- Apache Tomcat 5.5
- Nuance Imaging Framework Trace Service

- ShareScan Agent v5.0
- ShareScan Manager v5.0

There are other services which may not run by default, only if the respective functionality demands it:

- Nuance Documentum API
- Nuance MAPI-Process Starter
- Nuance Printer API
- S2D Inbox Agent

Tomcat service settings can be viewed/modified via:

```
%programfiles%\Apache Software Foundation\Tomcat 5.5\bin\tomcat5w.exe
```

During the entire installation process, do not remove the original installation media from your optical drive, even though the installer has already extracted and decompressed the required components to a temporary location. This action can cause multiple failures depending on the stage of the installation during which the removal happens.

6.2- Troubleshooting

If you experience an infinite rebooting loop on your target machine, look for and delete the following registry keys:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
```

```
Value: PendingFileRenameOperations
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update
```

```
Value: RebootRequired
```